ELEX MEDIA KOMPUTINDO

101 TIP & TRIK

Pemrograman PHP

- Mengungkap jenis-jenis attack terhadap aplikasi PHP, implementasinya, dan cara menanggulanginya.
- Menjelaskan strategi-strategi jitu untuk mempercepat eksekusi kode dan meningkatkan performansi aplikasi PHP.
- Pembahasan yang ringkas, jelas, dan komprehensif.

Didik Dwi Prasetyo

101 Tip & Trik Pemrograman PHP
Didik Dwi Prasetyo

Diterbitkan pertama kali oleh
Penerbit PT Elex Media Komputindo
Kelompok Gramedia, Anggota IKAPI, Jakarta 2006

121060468
ISBN: 979-20-8367-7

Cetakan ke-1: Februari 2006
Cetakan ke-2: Desember 2006
Cetakan ke-3: Januari 2008

Dicetak oleh Percetakan PT Gramedia, Jakarta
Isi di luar tanggung jawab percetakan

Daftar Isi

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Fungsi `print()` berperilaku seperti fungsi pada umumnya, dan memiliki nilai kembalian (*return value*) berupa integer 1. Dengan demikian, `print()` dapat digunakan sebagai bagian dari ekspresi yang lebih kompleks. Sementara itu, `echo()` mampu menerima lebih dari satu parameter sekaligus, dan tidak memiliki nilai kembalian.

```
print 'String 1';
echo 'String 1';
// Menggunakan beberapa parameter
echo 'String 1', "String 2", '...';
```

Fungsi string `echo()` akan dieksekusi lebih cepat dibanding dengan `print()`. Perbedaan ini disebabkan fungsi `print()` akan mengembalikan status (integer) yang menyatakan apakah proses berhasil dilaksanakan atau tidak.

Di sisi lain, `echo()` hanya menampilkan output saja dan tidak mengerjakan apa-apa lagi. Adapun dalam implementasinya, status nilai kembalian dari penggunaan fungsi string hampir tidak pernah diperlukan.

2

Deklarasi Variabel dan Variabel Dinamis

Tidak seperti bahasa lain (C, atau C++), variabel di PHP bisa digunakan meskipun belum dideklarasikan. Anda bisa menciptakan variabel kapan saja ketika memerlukan, kemudian menggunakannya. Variabel ini akan tetap eksis selama program dieksekusi.

Penamaan variabel harus diawali dengan tanda dollar ($) dan diikuti oleh nama ringkas. Nama variabel tidak boleh diawali

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
    if ($tNow > 17) return 'Good evening..';
}

// memanggil fungsi
echo greeting($time);
```

Dalam pengembangan aplikasi web, sebaiknya Anda menghindari penulisan ulang fungsi *pre-defined* PHP. Lain halnya jika fungsi Anda memiliki fungsionalitas khusus, dan penulisan ulang fungsi PHP diperlukan untuk mendukung implementasi fungsi. Contoh penulisan ulang fungsi PHP adalah seperti berikut:

```
// Menulis ulang fungsi strlen
function getLength($str) {
    return strlen($str);
}

// Mengembalikan panjang string
echo getLength('Hello');
```

Penulisan ulang fungsi-fungsi PHP mengakibatkan kode program susah dibaca oleh user. Disamping itu, yang lebih penting, penulisan ulang fungsi PHP di dalam fungsi *user-defined* akan memerlukan waktu tambahan saat eksekusi sehingga menjadikan kode lebih lambat.

5 Passing by Reference

Secara default, kita melewatkan (*passing*) argumen pada suatu fungsi menggunakan value. Mekanisme yang dikenal sebagai *passing-by-value* ini, pada teknisnya, meng-copy nilai argumen yang di-pass tersebut ke dalam variabel lokal.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
echo ('oke' = $pass2) ? 'OKE' : 'NOT OKE';
// Hasil: Pesan Error, kode tidak dieksekusi
```

Meskipun kode pada baris terakhir di atas akan menghasilkan pesan kesalahan ketika Anda keliru menuliskan operator komparasi, akan tetapi tidak sampai berakibat meloloskan string password yang tidak valid.

Alternatif lain untuk melakukan komparasi adalah menggunakan operator === (identik). Operator ini akan mengembalikan nilai true apabila operand yang dibandingkan memiliki nilai dan tipe sama. Ini berbeda sekali dengan operator ==, yang mengembalikan true jika nilai operand sama, meskipun tipe datanya berbeda. Contohnya seperti berikut:

```
$a = 123;     // integer
$b = '123';   // string

var_dump($a == $b);
// Hasil: bool(true)

var_dump($a === $b);
// Hasil: bool(false)
```

7 Tanda Kutip pada String

Parser PHP menentukan string-string dengan mencari pasangan tanda kutip. Oleh karena itu, semua string harus diawali dan diakhiri dengan tanda kutip yang sama, yaitu tunggal atau ganda. Apabila suatu string diapit oleh tanda kutip yang berbeda, parser PHP tidak akan menguraikan string tersebut.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
for ($i=0; $i<$n; $i++) {
        echo $arr[$i]. '<br>';
}
```

Walaupun pendekatan looping di atas cukup efisien, tetapi bisa tidak bekerja dengan baik ketika digunakan pada kasus array yang menggunakan key string, atau array di mana nilai key-nya tidak sekuensial. Sebagai solusinya, gunakan pernyataan `foreach`, seperti berikut:

```
$arr = array('PHP'        => 'Server-side',
             'JavaScript' => 'Client-side',
             'ASP'        => 'Server-side',
             'HTML'       => 'Client-side');

foreach($arr as $key => $val) {
   echo 'Key: ', $key, ' Value: ', $val, '<br>';
}
```

Ada kalanya, mungkin Anda perlu mengkonversi string ke array, dan sebaliknya, array ke string. Kasus ini bisa Anda selesaikan dengan mudah melalui fungsi `implode()` dan `explode()`. Contoh implementasinya seperti berikut:

```
// Konversi array ke string
$arr = array('PHP', 'JavaScript', 'ASP', 'HTML');
// Menggabung elemen array dengan string
$str = implode(', ', $arr);
echo 'String: ', $str;


// Konversi string ke array
$str = 'PHP, JavaScript, ASP, HTML';
// Split string dengan string ","
$arr = explode(',', $str);
echo 'Isi Array: <br>';

foreach($arr as $val) {
   echo $val, '<br>';
}
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

directive bisa diset saat runtime menggunakan `ini_set()`. Untuk lebih jelasnya bisa Anda lihat di dokumentasi PHP.

Apabila Anda hanya ingin mencari informasi konfigurasi directive tertentu tanpa mengubah nilainya, gunakan fungsi `ini_get()`. Adapun untuk semua konfigurasi, gunakan fungsi `ini_get_all()`.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
    <td>Your Name</td>
    <td><input type=text name="name"></td>
</tr>
</table>
<input type=submit name="oke" value="oke">
</form>
```

Untuk tujuan yang sama, selain menggunakan kombinasi `empty()` dan `trim()`, Anda juga bisa menggunakan kombinasi fungsi `strlen()` dan `trim()`. Contohnya seperti berikut:

```
if (strlen($name)=== 0) {
        echo 'isikan nama Anda...';
} else {
        echo 'okkay, ' .$name;
}
```

15 Casting Input Data

Pada saat Anda akan mengolah input data, pastikan bahwa input data tersebut sesuai dengan pola yang diizinkan. Langkah ini sangat diperlukan guna mencegah diprosesnya input data yang tidak valid atau kode program jahat. Adapun implementasinya adalah melakukan casting menggunakan operator casting.

Notasi operator casting sederhananya adalah tipe data yang ingin di-cast (dibungkus), dan diletakkan di dalam tanda kurung. Contohnya seperti berikut:

```
$a = '10ABC';
// casting $a ke integer
$b = (int)$a + (int)$a;
echo $b, '<br>';
// Hasil: 20
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
if (isset($_POST['oke'])) {
    if (isTgl($_POST['tgl']) &&
    isEmail($_POST['email'])) {
      echo 'input valid <br>';
      echo $_POST['tgl']. '<br>' .$_POST['email'];
    } else {
        echo 'input tidak valid';
    }
}
```

Fungsi `checkdate()` akan mengembalikan nilai true apabila nilai bulan adalah 1-12, tahun 1-32767, dan nilai hari menyesuaikan tahun serta bulan (mengacu kalender Gregorian). Dengan demikian, untuk dapat mengembalikan nilai true, maka input yang dimasukkan harus sesuai kalender. Ini bisa mencegah terjadinya ketidakcocokan antara input dari user Anda dan tanggal di kalender.

18 Pesan Error yang Praktis

Dalam membuat halaman pemrosesan form, sebaiknya Anda tidak memberikan pekerjaan ulang kepada user. Sebagai contoh, ketika user hanya melakukan kesalahan terhadap dua input, seharusnya input yang lain akan tetap ada dan nilainya tidak berubah.

Normalnya, pada saat ada satu atau beberapa input yang tidak valid, halaman form akan dikembalikan dalam keadaan kosong semua. Ini tentu kurang efektif dan efisien sehingga kita perlu mencari solusi yang lebih baik. Misalnya, dengan memberikan warna font mencolok pada field yang tidak valid, atau meletakkan pesan singkat di sebelah field terkait.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
// Verifikasi tgl
if (@$_POST['tgl'] && !isTgl($_POST['tgl']))
     $warnings['tgl'] = '<small>Tanggal Invalid';
// Verifikasi email
if (@$_POST['email'] && !isEmail($_POST['email']))
     $warnings['email'] = '<small>Email Invalid';
// Jika jumlah(count) warnings lebih dari 0
if (count(@$warnings) > 0) { ?>

<form action="<?$_SERVER['PHP_SELF']?>"
method=POST>
<table> •
<tr>
  <td>Tgl Lahir</td>
  <td><input type=text name="tgl"
     value="<?=@$_POST['tgl']?>"></td>
  <td><?=@$warnings['tgl']?></td>
</tr>
<tr>
  <td>Pekerjaan</td>
  <td><input type=text name="job"
     value="<?=@$_POST['job']?>"></td>
  <td></td>
</tr>
<tr>
  <td>Email</td>
  <td><input type=text name="email"
     value="<?=@$_POST['email']?>"></td>
  <td><?=@$warnings['email']?></td>
</tr>
</table>
<input type=submit value="Submit">
</form>

<?php
} else {     // count < 0
    echo 'Terima kasih... ';
} ?>
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

21 Membuat Form Smilies

Anda tentu tidak asing dengan smilies icon, bahkan mungkin sering menggunakannya ketika sedang chatting, posting, atau kirim email. Garis besar cara kerja form smilies adalah me-replace karakter-karakter khusus dengan ikon yang sesuai.

Solusi yang mudah untuk membuat form smilies adalah dengan mengimplementasikan array, kemudian memanfaatkan fungsi `str_replace()` yang sudah tersedia. Untuk menghindari ketidaksesuaian karakter dan ikon, Anda harus mendefinisikan terlebih dahulu karakter dan ikon yang akan digunakan. Contohnya seperti berikut:

```
<?php
$sm=array(
  ':)' => "<img src='img/smile.gif' border=0/>",
  ':(' => "<img src='img/sad.gif' border=0 />",
  ':D' => "<img src='img/biggrin.gif' border=0/>",
  ';)' => "<img src='img/wink.gif' border=0/>",
  ':?' => "<img src='img/question.gif' border=0/>",
  '8'  => "<img src='img/cool.gif' border=0/>",
  ':i' => "<img src='img/idea.gif' border=0/>" );
?>

<SCRIPT LANGUAGE='JavaScript'>
  <!-- function setIkon(ikon) {
       document.post.msg.value =
       document.post.msg.value + ikon;
  } //-->
</SCRIPT>

Click to add smiley
<?php // men-generate link ikon
    foreach ($sm as $key => $val) { ?>
    <a href="javascript:setIkon('<?=$key?>')"
    title="<?=$key?>"> <?=$val?> </a>
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

konteksnya agak berbeda, akan tetapi teknik dasarnya sangat mirip.

Dalam kasus spoofing form, penyerang meniru form Anda dan mengubah atau menghilangkan batasan-batasan yang telah Anda tetapkan. Dengan melakukan modifikasi ini, penyerang bisa leluasa mengirimkan paket data sesuai kehendaknya. Sebagai contoh, mengirim paket data dalam jumlah besar sehingga menghabiskan sumber daya. Teknik spoofing ini memang tidak memerlukan pengetahuan lebih bagi si penyerang.

Walaupun jenis penyerangan ini kelihatan sepele, akan tetapi terkadang tidak dapat kita cegah. Adapun solusi untuk mengatasinya adalah membuat proteksi pada form, khusnya form pemroses. Ini merupakan salah satu cara yang dianggap jitu guna melumpuhkan spoofing form. Sebagai contoh, ketika batasan paket data bisa lolos diinput form, Anda harus menambahkan kode untuk memeriksa ukuran paket data. Apabila paket data tidak valid, bisa dipastikan user tidak bisa mengirimkan paket data tersebut.

24

Hidden Field

Anda sebaiknya jangan pernah beranggapan bahwa field yang menggunakan tipe `HIDDEN` akan menjamin sekuriti. Kembali pada deskripsi dasarnya, tipe `HIDDEN` tidak merepresentasikan kontrol ke user, tetapi mengirimkan nilai dari properti `VALUE`. Meskipun nilainya tersembunyi, akan tetapi tidak aman untuk transfer data yang sifatnya sensitif, seperti password.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
        header('Location: ' .$_SERVER[PHP_SELF].
        '?myCookie=1');
        exit;

} else {  // Jika sudah di-set
        // Periksa apakah variabel sama
        if(isset($_COOKIE['myCookie'])) {
            setcookie('myCookie');
            echo 'OK, support cookie <br>';
            // print/debug cookie
            print_r($_COOKIE);
        } else {
            echo 'Tidak support cookie...!!';
        }
}
```

Cara kerja kode di atas sangat sederhana, dan terdiri atas dua tahap. Pertama, kode mencoba mengeset cookie dan me-redirect browser ke halaman yang sama, sambil menambahkan parameter `GET`. Kedua, begitu kode dieksekusi ulang, Anda tinggal memeriksa apakah nilai cookie tetap ada atau tidak.

27

Mengatasi Kegagalan Mengirim Cookie

Apakah Anda pernah mengalami kegagalan saat mengirim cookie? Misalnya, mendapat respon berupa pesan "*header already sent*" dari parser PHP. Ini berarti bahwa cookie yang Anda tetapkan tidak bisa dikirim dan diset.

Kegagalan seperti itu disebabkan karena kita terlebih dahulu mengirim output lain ke browser sebelum memanggil fungsi `setcookie()`. Contohnya seperti berikut:

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
session_start();
// Registrasi variabel session
$_SESSION['var_sess'] = 'Variabel Session';

// Menghapus variabel session
unset($_SESSION['var_sess']);

// Menghapus file session
session_destroy();
```

Pada kenyataannya, kedua kode di atas memiliki maksud dan tujuan yang sama. Meskipun demikian, disarankan Anda memilih pendekatan yang kedua.

30

Menyimpan Data Session

Secara default, data session akan disimpan pada file, di mana lokasinya ditentukan berdasarkan konfigurasi directive `session.save_handler` di php.ini. Konfigurasi ini sifatnya tidak mutlak, dengan demikian bisa Anda atur sendiri jika diperlukan.

Pengaturan lokasi penyimpanan session tidak harus dilakukan melalui file php.ini. Sebagai alternatif, Anda bisa menggunakan cara yang lebih praktis, yakni melalui fungsi `session_module_name()`. Fungsi ini mengizinkan Anda untuk menetapkan atau mendapatkan modul current session. Contoh pengaturannya seperti berikut:

```
// Menyimpan session di file (default)
session_module_name('files');

// Get module current session
echo session_module_name();
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

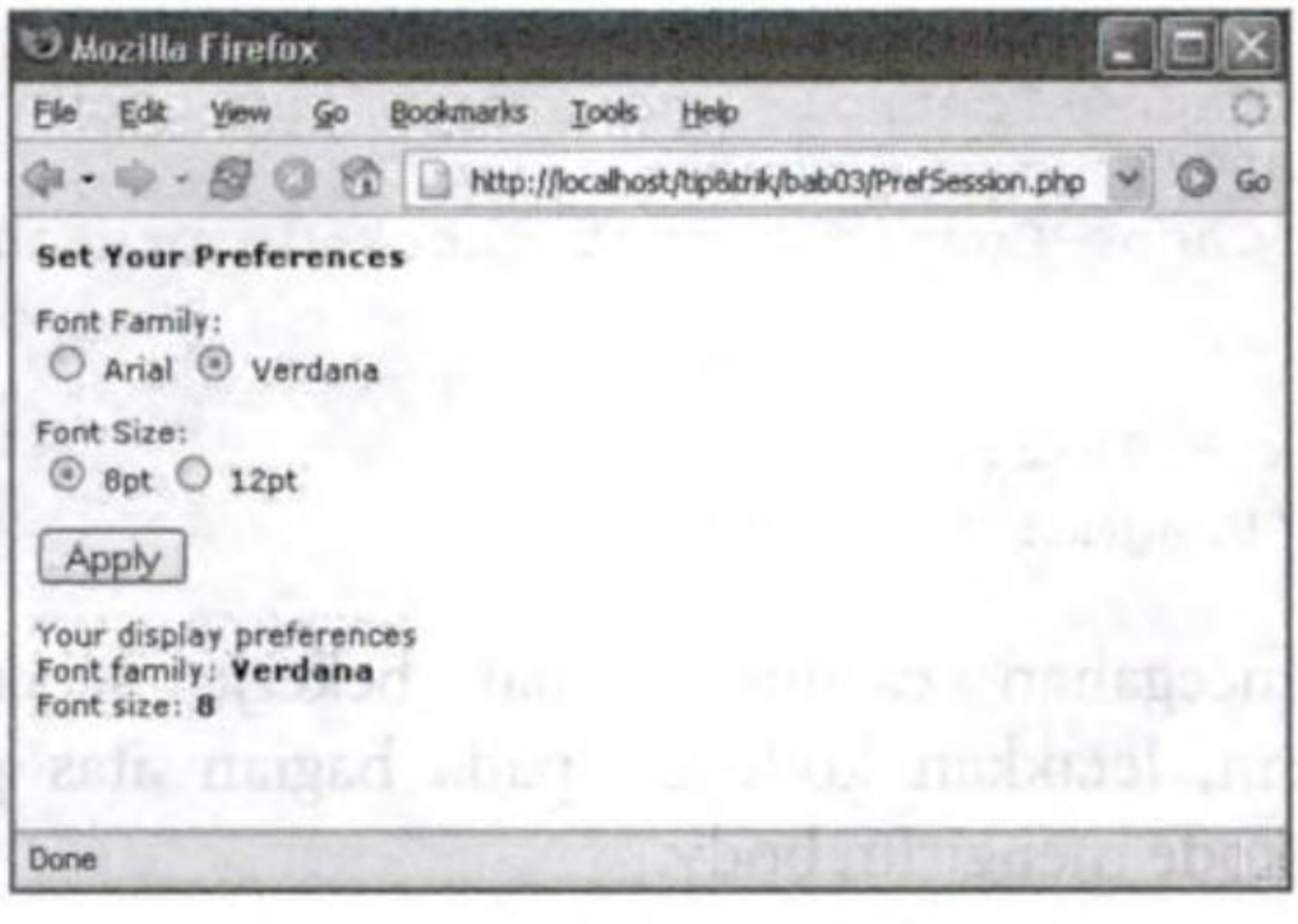
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
<input type="radio" name="ffamily" value="Arial">
Arial
<input type="radio" name="ffamily"
value="Verdana"> Verdana
<p>Font Size:<br>
<input type="radio" name="fsize" value=8> 8pt
<input type="radio" name="fsize" value=12> 12pt

<p><input type="submit" value="Apply"></p>
```

Agar informasi preferensi user bisa tersimpan secara permanen, gunakan file atau database untuk menampung data session.



Gambar 3.2 Mengatur preferensi tampilan user

33 Mencegah Cache Browser

Pada kenyataannya, mekanisme caching yang dilakukan oleh browser dapat meningkatkan akses halaman web. Di mana ketika Anda mengetikkan alamat URL, pertama kali browser akan memeriksa cache-nya guna melihat apakah halaman sudah pernah dikunjungi atau belum. Jika ternyata sudah

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

sini penyerang melakukan aksinya setelah user login ke komputer server. Sebenarnya, serangan ini juga ada kaitannya dengan session fixation.

Pendekatan yang baik untuk mencegah session hijacking adalah dengan menyebarkan token. Langkah ini harus didukung dengan penggunaan algoritma hashing atau enkripsi. Contohnya seperti berikut:

```
session_start();

$token = md5($_SERVER['HTTP_ACCEPT_ENCODING']
             . $_SERVER['HTTP_ACCEPT_LANGUAGE']
             . $_SERVER['HTTP_USER_AGENT']);

if (isset($_SESSION['HTTP_USER_AGENT'])) {
    if ($_SESSION['HTTP_USER_AGENT'] != $token) {
        exit('Invalid...');
    }

} else {
    $_SESSION['HTTP_USER_AGENT'] = $token;
}

// print/debug session
print_r($_SESSION);
```

Perlu diketahui, keamanan data session tidak hanya dipengaruhi oleh teknik hashing ataupun enkripsi. Ada faktor lain yang perlu Anda perhatikan, yaitu lokasi penyimpanan session. Di mana normalnya terletak di direktori temporary (tmp). Pastikan bahwa direktori ini tidak bisa diakses oleh user lain. Akan lebih baik lagi jika session ditempatkan di memori, dengan mengatur konfigurasi directive `session.save_path`, dan memberinya nilai mm.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
 */
function myMagic($str) {
    // Jika magic quote gpc On, stripslashes
    if (get_magic_quotes_gpc()) {
        $str = stripslashes($str);
    }
    // Strip tag HTML
    $str = strip_tags(trim($str));
    // Escape karakter spesial
    return mysql_real_escape_string($str);
}
```

Apabila Anda bekerja dengan database server lain yang tidak menyediakan fungsi dedicated, seperti Microsoft SQL Server, Sybase, mSQL, dan Oracle, gunakan fungsi `addslashes()`.

```
function myMagic2($str) {
    if (get_magic_quotes_gpc($str)) {
        $str = stripslashes($str);
    }
    $str = strip_tags(trim($str));
    return addslashes($str);
}
```

Untuk menjaga keamanan sistem aplikasi web Anda, jangan pernah menjalankan input query tanpa di-filter terlebih dahulu. Khususnya adalah input yang dikirim melalui method `POST` atau `GET`.

38

Master-Detail

Apabila Anda sudah memahami kunci dasar hubungan master-detail, tidak akan sulit untuk mengimplementasikan ke dalam kode program. Dalam hubungan master-detail, sebuah tabel bertindak sebagai master, dan tabel lainnya

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

niknya, melakukan penulisan bersamaan dengan data di-retrieve dari database. Kode programnya seperti berikut:

```
<?php
/* DumpCSV.php */

$file = 'C:/temp/data.csv';
$db  =  mysqli_connect('localhost',  'didik',  '',
'mydb');
$sql   =   'SELECT   kode,   judul,   pengarang,
id_penerbit, tahun FROM buku';
$res = mysqli_query($db, $sql);
?>

<table width=500 border=1>
<tr>
   <td>Kode</td><td>Judul</td><td>Pengarang</td>
   <td>Penerbit</td><td>Tahun</td>
</tr>

<?php
$csv = '';
if ($res != null) {
   while ($row = mysqli_fetch_row($res)) {
      echo '<tr><td>' .$row[0]. '</td>
      <td>' .$row[1]. '</td> <td>' .$row[2].
      '</td><td>' .$row[3]. '</td>
      <td>' .$row[4]. '</td></tr>';
      // Mengembalikan string dari elemen array
      // glue/delimeter string adalah titik koma
      $csv.= implode(';', $row)."\n";
}
echo '</table> <br>';
mysqli_free_result($res);
// Membuka file untuk operasi penulisan saja
$fp = fopen($file, 'w')
or die('Tidak bisa membuka file '.$file);
// Menulis string ke file
$fw = fwrite($fp, $csv);
fclose($fp);
// buat link, jika berhasil menulis file
if ($fw) {
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
$db  =  mysqli_connect('localhost',  'didik',  '',
'mydb');
$sql  =  'SELECT  kode_buku,  judul,  pengarang,
penerbit, tahun FROM buku ORDER BY kode_buku';
$res = mysqli_query($db, $sql);

if ($res != null) {
    $jml = mysqli_num_rows($res);
    if ($jml == 0) {
        echo 'Tabel kosong';
        exit;
    }
    // Batas baris per halaman
    $batas = 4;
    if (($jml%$batas) == 0) {
        $jmlpage = (int)($jml/$batas);
    } else {
        $jmlpage = ((int)$jml/$batas)+1;
    }
    // Inisialisasi variabel page
    (isset($_GET['page'])) ?
    $page = (int)$_GET['page'] : $page =1;
    if ($page > $jmlpage)
        $page=$jmlpage;

    while ($rows = mysqli_fetch_array($res)) {
        $arrdata[]=$rows;
    }
    mysqli_free_result($res);
    mysqli_close($db);

    // Set end dan start page
    $end  = (int)($page*$batas)-1;
    $start= (int)$end-($batas-1);
    if ($end>$jml)
        $end=$jml-1;
    for ($i=$start; $i<=$end; $i++) {
        $arr[] = $arrdata[$i];
    }
    ?>
    <center><table width=400
    style="border:1pt solid #666666;">
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

prinsipnya, untuk dapat melakukan transaksi dengan baik, Anda harus menggunakan tipe tabel yang mendukung transaksi, yaitu innodb, atau bdb.

```
$sql = 'SHOW VARIABLES LIKE "have_innodb"';
if ($res = mysqli_query($db, $sql)) {
    while ($row = mysqli_fetch_row($res)) {
        echo $row[0], ': ', $row[1];
    }
    mysqli_free_result($res);
}
```

Apabila hasil query mengembalikan nilai Yes, berarti tabel untuk transaksi sudah aktif dan bisa digunakan. Langkah selanjutnya, buat tabel dengan menetapkan tipe tabel sebagai innodb. Perlu diketahui juga, secara default MySQL menerapkan mode auto-commit pada tabel transaksi. Jika Anda tidak menginginkan, ubah mode ini sebelum transaksi dilakukan. Caranya seperti kode program berikut:

```
// set autocommit Off
mysqli_autocommit($db, FALSE);
$sql = "INSERT INTO myInnoDB VALUES
        (1, 'guest'),
        (2, 'user'),
        (3, 'admin')";
// insert rows
if ($res = mysqli_query($db, $sql)) {
    printf("%d rows di-insert <br>\n",
    mysqli_affected_rows($db));
    mysqli_free_result($res);
}
// commit transaksi (insert)
mysqli_commit($db);
echo 'commit transaksi <br>';

if ($res = mysqli_query($db,
'SELECT id FROM myInnoDB')) {
    $jml = mysqli_num_rows($res);
    printf("%d rows in table <br>", $jml);
    mysqli_free_result($res);
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
sqlite_create_function($db,  'mySUM',  'sqliteSum',
2);

$arr = sqlite_array_query($db,
'SELECT bil1, bil2, mySUM(bil1, bil2) AS sum FROM
test', SQLITE_ASSOC);

foreach ($arr as $row) {
   $x = 'bil1: ' .$row['bil1']. ', ';
   $x .= ' bil2: ' .$row['bil2']. ' -> ';
   $x .= ' sum: '. $row['sum']. '<br>';
   echo $x;
}
```

46

Mencegah SQL Injection

SQL injection adalah salah satu jenis penyerangan yang mengizinkan user tidak sah (penyerang) untuk mengakses database server. Pada dasarnya, serangan ini difasilitasi oleh kode program Anda sendiri. Tekniknya, penyerang mencoba memasukkan query (melalui field atau URL) yang akan menyebabkan database server men-generete query SQL yang tidak valid.

Pada kenyataannya, SQL Injection terbukti merupakan salah satu teknik terbaik yang sering melumpuhkan sasarannya. Begitu penyerang berhasil menguasai kendali database server, ia bisa melakukan apa saja, seperti memodifikasi atau bahkan menghapus semua data yang ada. Bagaimanapun juga, ini bisa dicegah jika kode program Anda melakukan validasi dengan baik.

Sebenarnya, apabila Anda teliti, teknik SQL injection sangat sederhana sekali. Akan tetapi, justru ini yang sering diabaikan oleh para pemrogram, entah itu karena tidak tahu atau lupa.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

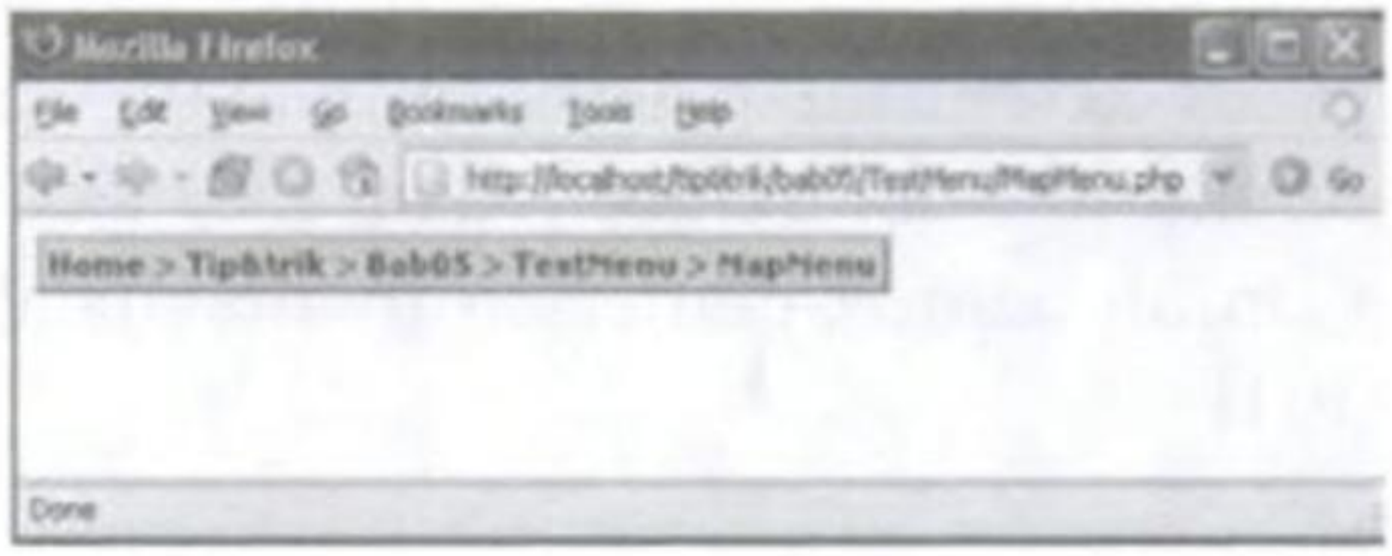
```
}
// Membebaskan memori
$res->free();
// Menutup koneksi
$db->disconnect();
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
    // Set kapital tiap awal kata (word)
    $path[$i] = ucwords($path[$i]);
    echo ' > <a href=' .$urlbase. '>' .$path[$i].
'</a>';
}
echo '</td></tr></table>';
```



Gambar 5.1 Memetakan file dan direktori

50
Menu Tab

Di tool-tool RAD (*Rapid Application Development*), seperti Visual Basic dan Borland Delphi, Anda pasti mengenal komponen tab atau tabbed pane. Keberadaan tab ini menjadikan aplikasi desktop lebih praktis dan memiliki tampilan yang menarik.

Begitu pula halnya dengan aplikasi web, tab memiliki fungsionalitas sama, meski implementasinya berbeda. Sebenarnya tidak terlalu rumit untuk mengimplementasikan tabbed pane di halaman web. Anda bisa memanfaatkan elemen `<TABLE>` untuk mendesain halaman menu yang merepresentasikan tabbed pane. Lebih jelasnya, perhatikan kode program berikut:

```
$menu = array(
    'Tutorials' => 'tutorials.php',
    'Article'   => 'article.php',
    'News'      => 'news.php',
```

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

101
TIP & TRIK

Buku ini mencoba menyajikan materi yang komprehensif mengenai pemrograman aplikasi web dengan PHP. Materi yang dikemas rapi dalam tip dan trik ini didesain agar mudah dipahami dan diimplementasikan.

Beberapa topik yang diungkap, antara lain:

- Bagaimana menulis kode program PHP yang efektif dan efisien?
- Bagaimana melakukan pemrosesan form yang baik, sekaligus cara mencegah XSS dan CSRF attack?
- Cara mengolah database dengan cepat, membuat cache query/result, mencegah Command dan SQL Injection.
- Manajemen image, file, flushing dan buffering output menggunakan PHP.
- Bagaimana cara men-debug, mengoptimasi, dan meningkatkan performansi aplikasi-aplikasi PHP?
- Bagaimana mendesain aplikasi PHP yang memiliki sekuritas tinggi?

Setelah membaca buku ini, Anda akan mengetahui solusi yang lebih banyak untuk mengembangkan aplikasi web dengan PHP. Tentunya Anda tidak ingin mempersulit diri dengan memilih solusi yang rumit, jika ada cara lain yang lebih praktis dan efisien.

Tentang Penulis

Didik Dwi Prasetyo, adalah programmer freelance yang sangat tertarik mendalami bidang aplikasi internet dan database.
Email penulis: **didik_rpl@yahoo.com**

Kelompok
Pemrograman
Ketrampilan
☑ Tingkat Pemula
☑ Tingkat Menengah
☐ Tingkat Mahir
Jenis Buku
☐ Referensi
☑ Tutorial
☐ Latihan

ISBN 979-20-8367-7
9 789792 083675
EMK 121060468

Penerbit PT Elex Media Komputindo
Jl. Palmerah Selatan 22, Jakarta 10270
Telp. (021) 5483008, 5490666, 5480888
Ext. 3323
Web page: http://www.elexmedia.co.id